PCT/ZA2004/00072

Sertifikaat

REPUBLIEK VAN SUID AFRIKA

Certificate

REPUBLIC OF SOUTH AFRICA

PATENT KANTOOR
DEPARTEMENT VAN HANDEL
EN NYWERHEID

PATENT OFFICE
DEPARTMENT OF TRADE AND
INDUSTRY

Hiermee word gesertifiseer dat
This is to certify that

the documents annexed hereto are true copies of:

Application forms P.1, P2 and provisional specification and drawings of South African Patent Application No. 2003/5129 as originally filed in the Republic of South Africa on 30 June 2003 in the name of ADELE KATRINE NARAINSAMY and an applicant substituted to SELVANATHAN NARAINSAMY on 15 June 2004 for an invention entitled: " GSM TRANSACTION MANAGEMENT SYSTEM".

Geteken te PRETORIA in die Republiek van Suid-Afrika, hierdie 2 dag van December 2004
Signed at PRETORIA in the Republic of South Africa, this 2 day of December 2004

Registrar of Patents

REPUBLIC OF SOUTH AFRICA

FORM P2

PATENTS ACT, 1978

REGISTER OF PATENTS

Official number		**Lodging date - provisional**		**Acceptance date**	
21	2003/5129	22	30 June 2003		
International classification		**Lodging date - complete**		**Grant date**	
51		23		47	

Full name(s) of applicant(s)/patentee(s)

71	Adele Katrine Narainsamy

Applicant(s) substituted		**Date registered**
71	SELVANATHAN NARAINSAMY	15.06.04

Assignment - Assignee(s)		**Date registered**
71		

Full name(s) of inventor(s)

71	Adele Katrine Narainsamy

Priority claimed	**country**		**number**		**date**	
	33		31		32	
	33		31		32	
	33		31		32	

Title of the invention

54	GSM Transaction Management System

Addresses of applicant(s)/patentee(s)

Suite 903,Tower B, Salisbury Centre, 349-351 West Street, Durban, 4001

74 **Address for service**

PFT Burger reference: **PP.3740.NAR**

PFT Burger, Patent & Trade Mark Attorneys
10 Mount Argus Road, Umgeni Heights, Durban - PO Box 546, Durban 4000
DOCEX 305 DURBAN
TEL - 573 1054 FAX - 573 1058

Patent of addition - no.		**Date of any change**
61		
Fresh application based on:		**Date of any change**

REPUBLIC OF SOUTH AFRICA
PATENTS ACT, 1978
Application for a patent and acknowledgement of receipt
[section 30(1) - regulation 22]

FORM P1

Official number		
21	01	2003/5129

PFT Burger reference
PP.3740.NAR

71. Full name(s) of applicant(s) ~~Adele Katrine Narainsamy~~ SELVANATHAN NARAINSAMY

Address(es) of applicant(s) Suite 908, Tower B, Salisbury Centre, 349-351 West Street, Durban, 4001

54. Title of the invention

GSM Transaction Management System

☒ The applicant claims the priority set out on the enclosed Form P2

21. 01. This application is for a patent of addition to Patent Application no.

21 01 This application is a fresh application in terms of s37 and is based on Patent Application no.

This application is accompanied by:

1 A single copy of a provisional two copies of a complete specification of 8 pages

2 Drawings of 2 sheets

74 Address for service

PFT Burger, Patent & Trade Mark Attorneys
10 Mount Argus Road, Umgeni Heights, Durban - PO Box 546, Durban 4000
DOCEX 305 DURBAN
TEL - 573 1054 FAX - 573 1058

Dated: 30 June 2003

PFT Burger, Patent & Trade Mark Attorneys

RECEIVED
Official date stamp

Registrar of Patents

REPUBLIC OF SOUTH AFRICA
PATENTS ACT, 1978
Provisional specification
[section 30(1) - regulation 27]

FORM P6

Official number		
21	01	2003/5129

Lodging date	
22	30 June 2003

Full name(s) of applicant(s)	
71	Adele Katrine Narainsamy

Full name(s) of inventor(s)	
72	Adele Katrine Narainsamy

Title of the invention	
54	GSM Transaction Management System

PFT Burger reference: - PP.3740.NAR

Background to the invention

This invention relates to a method of processing a transaction, particularly a financial transaction by means of a personal communication device.

The invention will be described with reference to the use of a cellular telephone or mobile telephone as the personal communication device. In addition, the invention will be described with reference to a point of sale (POS) terminal or an automated teller machine (ATM) as a transaction terminal. This is done purely by way of example and it is not intended thereby to limit the invention.

Summary of the invention

This invention provides a method of processing, by means of a personal communication device and a transaction terminal remote therefrom, a transaction involving a remote transaction processing authority, the method comprising the steps of:

with the use of the personal communication device, formulating and encrypting, by means of a first encryption key and a code unique to the personal communication device, a transaction request to be transmitted to the transaction terminal and transmitting the transaction request to the transaction terminal;

transmitting the transaction request from the transaction terminal to the transaction processing authority;

at the transaction processing authority, receiving the transaction request and identifying the personal communication device using the code unique to the personal communication device, retrieving the first encryption key, previously stored at the transaction processing authority in respect of the personal communication device, decrypting the encrypted transaction request using the first encryption key, processing the transaction request and generating a process outcome message pertaining to the result of processing of the transaction request, generating a second encryption key, storing the second encryption key in the transaction processing authority, transmitting the second encryption key to the transaction terminal, encrypting the process outcome message using the second encryption key and transmitting the encrypted process outcome message to the personal communication device;

within the personal communication device, extracting and storing the second encryption key and transmitting the encrypted process outcome message to the transaction terminal; and

at the transaction terminal, decrypting the encrypted process outcome message and applying the decrypted process outcome message to actuate the transaction terminal.

The second encryption key that is stored at the transaction processing authority and in the personal communication device may be used, in a following transaction processing cycle as the first encryption key.

The second encryption key is preferably generated, every time the transaction processing cycle is repeated, with the use of code hopping techniques.

Code hopping is facilitated by the fact that the second encryption key is stored, both at the transaction processing authority and within the personal communication device, since this assists in synchronising the constantly changing keys.

In the process of encrypting the transaction request to be transmitted to the transaction processing authority the transaction request may conveniently be encrypted with the use, in addition to one or more of the first encryption key, a code unique to the personal communication device and transaction request data, of a code, such as a personal identification number (PIN), unique to the person requesting the transaction.

To simplify and speed up processing, the identity code of the personal communication device may conveniently be sent in clear text whenever it is sent. This will facilitate identification of the personal communication device and speed up decryption at the point of reception of the information concerned.

The personal communication device may conveniently be constituted by a cellular telephone and the preferred form of communication between the personal communication device and the transaction terminal is by way of a short range link, preferably an infrared link. This will add to the security of the system.

The transaction terminal may be constituted by any piece of equipment capable of receiving communications from the personal communication device and performing a function in response to a request from the device. Examples of such transaction terminals are automated teller machines (ATMs), point of sale (POS) terminals and the like.

The transaction terminal need not be limited to a financial transaction processing machine. For instance, the transaction terminal could be a door or a gate that is opened in response to a signal from the personal communication device.

The transaction processing authority will depend on the transaction termi8nal involved. If the transaction terminal is an ATM, then the transaction processing authority will be a bank or other financial institution. If the transaction terminal is a door or a gate, then the transaction processing authority might conveniently be constituted by the security system of the premises concerned.

The invention includes apparatus and equipment adapted for implementation of the method of the invention.

Brief description of the drawings

The invention will be further described with reference to the accompanying drawings in which:

Figure 1 is a block diagram illustrating apparatus for implementing the method of the invention;

Figure 2 is a block diagram illustrating (partly in flow-chart form), one implementation of the method of the invention.

Description of embodiments of the invention

The system 10 illustrated in figure 1 is a transaction processing system that utilises a cellular telephone 12 to communicate with a POS terminal or ATM 14. Transactions requested within the transaction processing system 10 will require authorisation by a transaction processing authority constituted, in this case, by a financial services provider 16. For ease of reference, the transaction terminal will be taken to be an ATM.

Communications between the ATM 14 and the financial services provider 16 are by way of a GSM communicator 18. Alternatively or in addition, communication between the ATM 14 and the financial services provider 16 may take place on conventional communication networks incorporating the ATM 14, such as a conventional telephone network.

To enhance the security of the transaction processing system 10, communications between the cellular telephone12 and the ATM 14 are by way of very short range communications links. Most cellular telephones are equipped with infrared transceivers 20. Infrared is a relatively secure form of short range communication. The ATM 14 can be fitted with an infrared transceiver 22 relatively simply.

A person wishing to initiate a transaction simply enters the transaction details on the cellular telephone 12 and, using the appropriate features on the telephone, transmits a first infrared signal 24 to the ATM 14.

This process is best illustrated with reference to Figure 2.

As can be seen from Figure 2, a person wishing to initiate a transaction starts off by entering transaction data (D_{Trr}) into the telephone 12. Upon registration within the transaction processing system 10, the person concerned will have been issued with a personal identification number (PIN) and at this point the person will be prompted to enter the PIN as data (D_{PIN}) into the cellular telephone 12. Within the cellular telephone 12, the data so entered (D_{Trr} and D_{PIN}) will be encrypted using a first encryption key (K1) as well as the identification number (ID) of the telephone 12 (which may be a manufacturer's serial number or some other telephone identification number allocated upon registration within the system 10) and the data previously entered (D_{PIN} and D_{Trr}). Not all of this information needs to be used in preparing the encrypted transaction request – E(D_{Trr}).

The encrypted transaction request (E(D_{Trr})) is then transmitted to the ATM 14 by way of a first infrared transmission 24. The telephone ID can be sent as clear text.

On receipt within the ATM 14, the encrypted transaction request (E(D_{Trr})) together with the telephone ID is transmitted by way of a transmission 26 to the financial services provider 16.

The message received at the financial services provider 16 (E(D_{Trr}):ID) must now be decrypted.

The financial services provider 16 has data pertaining to the user and the telephone 12 stored in its databases, which data is linked to the telephone 12 by way of the telephone ID, the most important being data pertaining to the user's PIN (D_{PIN}) and the first encryption key (K1). The manner in which encryption keys are generated and stored will be described in more detail below.

On receipt of the encrypted transaction request ($E(D_{Trr})$:ID), the financial services provider 16 retrieves this stored data and, using this data (particularly K1:D_{PIN}) it is able to decrypt the encrypted transaction request ($E(D_{Trr})$)and to process the transaction request.

The outcome of this process will either be positive (for instance to dispense funds or to display account information) or there will be some other outcome (for instance, not to dispense funds or not to display account information, transfer funds or some other message).

The process outcome message must be communicated both to the person requesting the transaction and to the ATM 14, since the ATM 14 in particular will be required to perform certain functions in response thereto. In view of the potential sensitivity of this information, this information is encrypted.

The process of encryption is undertaken by the financial services provider which generates a second encryption key (K2). The second encryption key (K2) is stored in the databases of the financial services provider 16 and linked to the telephone ID to facilitate future retrieval of the key. The second encryption key (K2) or a derivative thereof will be used as the decryption key (K1) in the next transaction processing cycle.

Assuming that the transaction is authorised, the financial services provider generates a transaction authorisation message (D_{Tra}). The financial services provider 16 encrypts the transaction authorisation message (D_{Tra}) using the second encryption key (K2) and other data typically the telephone ID, the PIN number (D_{PIN}) and the data pertaining to the transaction authorisation message (D_{Tra}).

The encrypted transaction authorisation message ($E(D_{Tra})$) is then transmitted to the telephone 12 by way of the GSM network, the most convenient form of transmission being as a Short Message Service (SMS) message 28. At the same time, the financial services provider 16 transmits the second encryption key ((K2)) to the ATM 14, by way of a communication 30 between the financial services provider 16 and the ATM 14.

On receipt within the telephone 12, the encrypted transaction authorisation message ($E(D_{Tra})$) is transmitted to the ATM 14 by way of a second infrared message 32.

Within the ATM 14 the encrypted transaction authorisation message (E(D_{Tra})) is decrypted using the second encryption key (K2) received from the financial services provider 16. The second encryption key (K2) is transmitted to the telephone 12 as part of the infrared communication 32 and the decrypted transaction authorisation message (D_{Tra}) is used to direct the operation of the ATM 14. In this example, the ATM 14 is instructed to dispense funds to the person who originally requested the transaction.

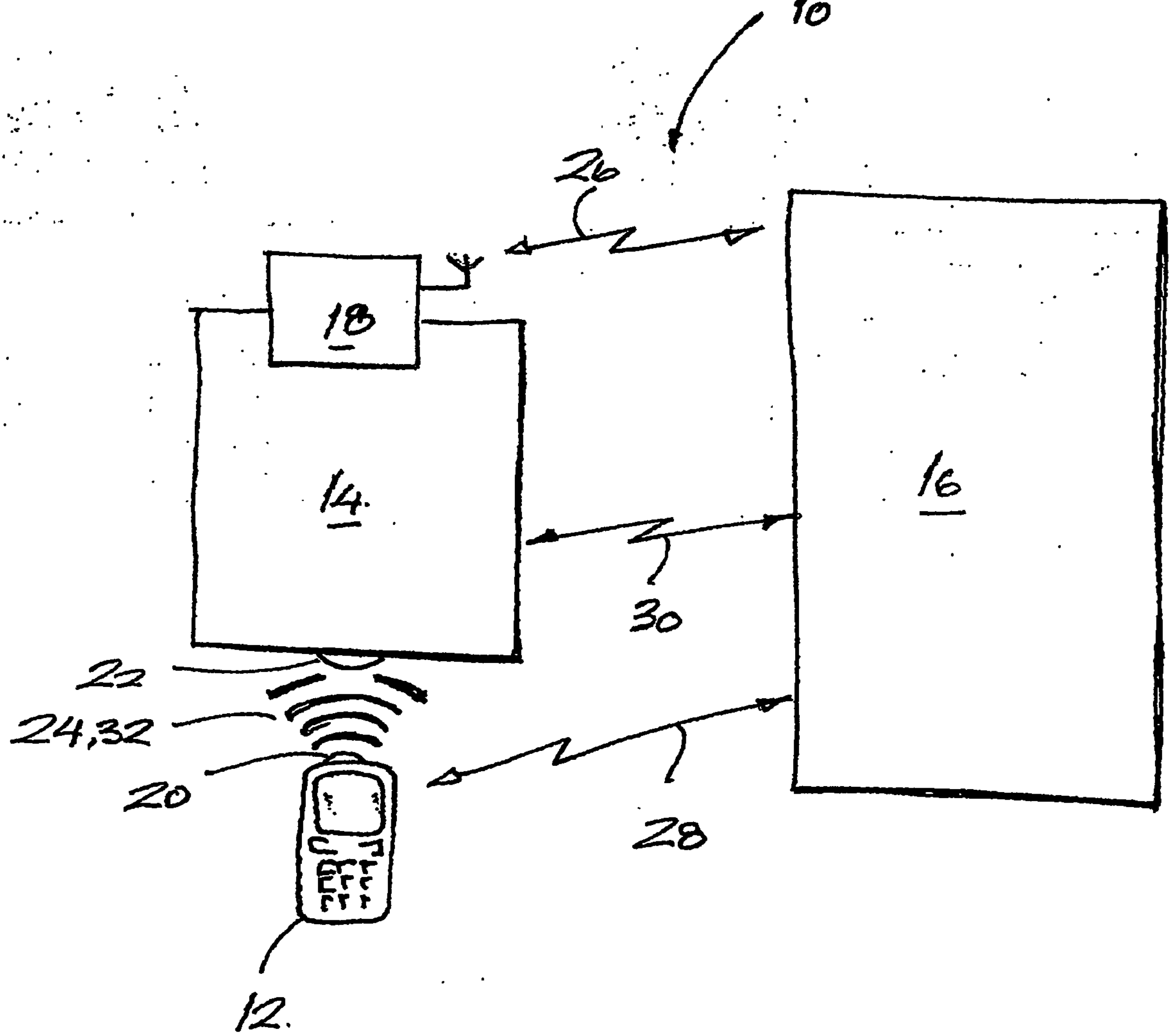
Within the telephone 12, the second encryption key (K2) is now stored in a database. When next the person wishes to commence a transaction processing cycle, the second encryption key (K2) stored in the telephone database is used as the initial encryption key (K1) in that next transaction. The second encryption key (K2) stored at the financial services provider 16 will then be used as a decryption key and a new second encryption key (K2) will be generated in that next transaction. In this manner, the encryption keys are kept in synchronicity. A number of methods are known within code hopping techniques to ensure that security is maintained and replay attacks are avoided. In addition, techniques are known to ensure that key synchronisation remains possible in the event that an abortive process results in possible key mismatch.

The financial transaction process related above is but one example of the transaction processing capacity of the system.

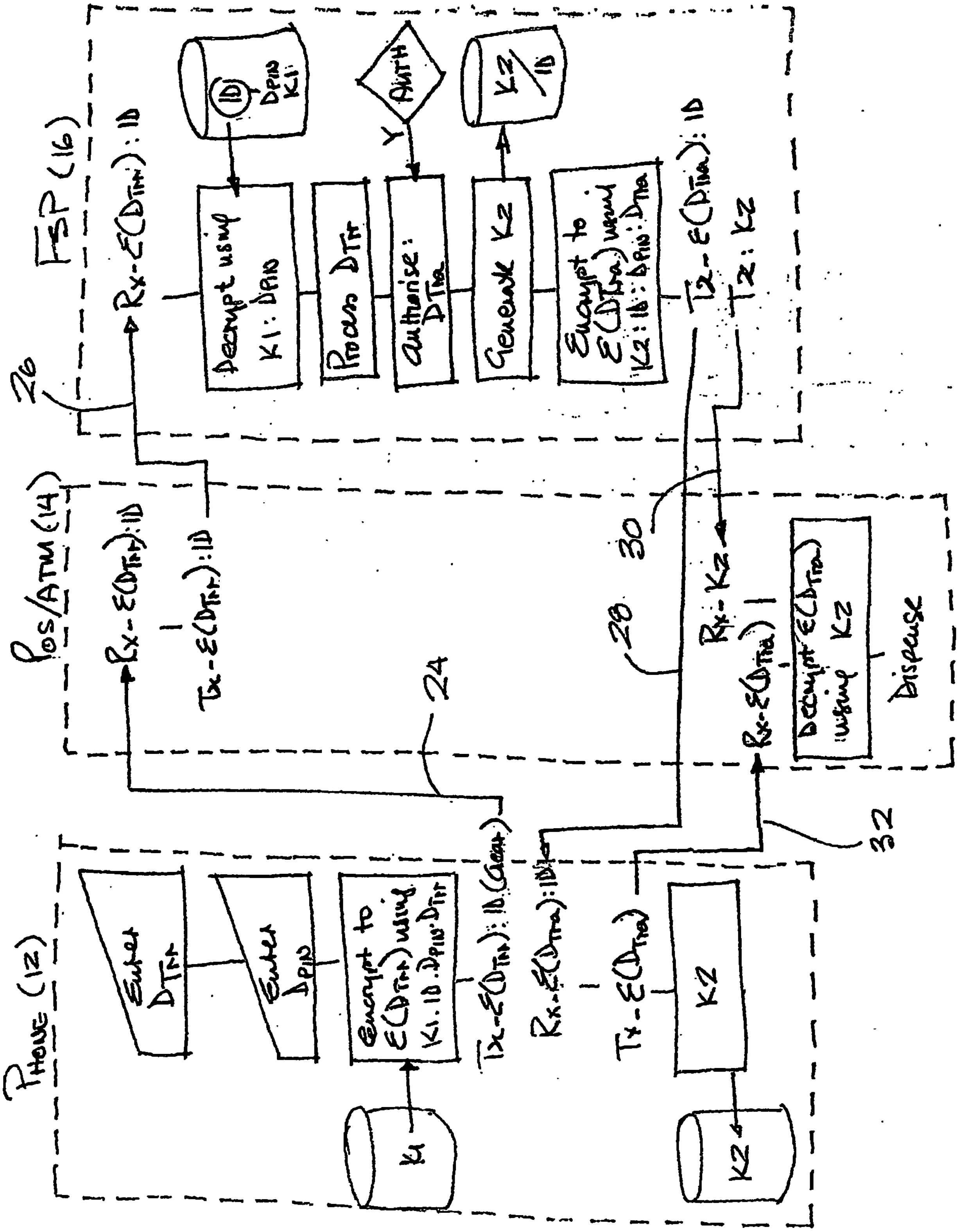
Dated 27 June 2003

....

PFT Burger Patent & Trade Mark Attorneys
Applicant's Patent Attorneys



PFT Burger, Patent and Trade Mark Attorneys
Applicant's Patent Attorneys


FSP (16)
Rx-E(D_TRA):ID
Decrypt using K1:D_PIN
ID
D_PIN K1
Process D_TR
Authorise: D_TRA
AUTH
Y
Generate K2
K2
ID
Encrypt to E(D_TRA) using K2:ID:D_PIN:D_TRA
Tx-E(D_TRA):ID
Tx:K2
26
POS/ATM (14)
Rx-E(D_TRA):ID
Tx-E(D_TRA):ID
30
Rx-K2
28
Rx-E(D_TRA)
Decrypt E(D_TRA) using K2
Dispense
24
32
Phone (12)
Enter D_TR
Enter D_PIN
Encrypt to E(D_TRA) using K1.ID.D_PIN.D_TR
Tx-E(D_TRA):ID (Clear)
Rx-E(D_TRA):ID
Tx-E(D_TRA)
K2
K1
K2

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/ZA04/000072

International filing date: 30 June 2004 (30.06.2004)

Document type: Certified copy of priority document

Document details: Country/Office: ZA
Number: 03/5129
Filing date: 30 June 2003 (30.06.2003)

Date of receipt at the International Bureau: 28 January 2005 (28.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse